Practicals on VOMS and MyProxy

Emidio Giorgio

INFN

Retreat between GILDA and ESR VO, Bratislava, 27-30.06.2005

Outline

- VOMS vs. plain proxy
- VOMS proxy creation
- MyProxy
- Obtaining VOMS delegation through MyProxy

VOMS generalities

- Virtual Organisation Membership Services is service which keeps track of VO members and grants users authorization to access resources at the VO level
- Differently from standard plain proxies, provides support for group membership, roles, and capabilities
- Each VO has a server, which is contacted from user when he initializes his voms-proxy
- VOMS server returns a proxy, containing also infos on user (Attribute Certificate), which are included in a unique certificate

VOMS proxy creation

- **voms-proxy-init --voms gildav**

```
Your identity: /C=IT/O=GILDA/OU=Personal
  Certificate/L=INFN/CN=Emidio
  Giorgio/Email=emidio.giorgio@ct.infn.it
Enter GRID pass phrase for this identity:
[insert your certificate passphrase]
Creating temporary proxy
  ..................................... Done
/C=IT/O=INFN/OU=Host/L=CNAF/CN=cert-voms-
  01.cnaf.infn.it
/C=IT/O=INFN/CN=INFN Certification Authority
Creating proxy
..................................... Done
Your proxy is valid until Mon Jun 13 09:06:00 2005
```

VOMS proxy creation

- **Principal options**
  - -hours x, create a proxy valid for x hours
  - -vomslife x, create a proxy with AC valid for x hours
  - -cert <certfile> Non-standard location of user certificate
  - -key <keyfile> Non-standard location of user key
  - -out <proxyfile> Non-standard location of new proxy cert

- **Default** maximum value for vomslife is 24, superior requests will be shortened to 86400 seconds (24 h)

Verify your credentials

- `voms-proxy-info`

- **Principal options :**
  -all prints all proxy options
  -file specifies a different location of proxy file

WARNING : in gLite 1.0, you may have problems (error 5025) with glite-job-* commands, when in /etc/grid-security/vomsdir there's more than one host certificate. By pass this creating a directory containing only the host certificate of your VOMS server.

```
[giorgio@glite-tutor:~]$ ls /etc/grid-
   security/vomsdir.gildav.glite/
 gildav-cert-voms-01.cnaf.infn.it.pem
```

Then

```
export X509_VOMS_DIR=/etc/grid-
  security/vomsdir.gildav.glite/
```

Verify obtained credentials

```
[giorgio@glite-tutor:~]$ voms-proxy-info --all
subject   : /C=IT/O=GILDA/OU=Personal
   Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it/CN=proxy
issuer    : /C=IT/O=GILDA/OU=Personal
   Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it
identity  : /C=IT/O=GILDA/OU=Personal
   Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it
type      : proxy
strength  : 512 bits
path      : /tmp/x509up_u513
timeleft  : 20:59:53
VO        : gildav
subject   : /C=IT/O=GILDA/OU=Personal
   Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it
issuer    : /C=IT/O=INFN/OU=Host/L=CNAF/CN=cert-voms-
   01.cnaf.infn.it
attribute : /gildav/Role=NULL/Capability=NULL
timeleft  : 20:58:28
```

Long term proxy : MyProxy

- **Proxy (and VOMS proxy) have limited lifetime (default is 12 h)**
  - Bad idea to have longer proxy
- **However, a grid task might need to use a proxy for a much longer time**
  - Grid jobs in HEP Data Challenges on LCG last up to 2 days
- **myproxy server:**
  - Allows to create and store a long term proxy certificate:
  - myproxy-init -s <host_name>
    - -s: <host_name> specifies the hostname of the myproxy server
  - myproxy-info
    - Get information about stored long living proxy
  - myproxy-get-delegation
    - Get a new proxy from the MyProxy server
  - myproxy-destroy
  - Check out the myproxy-xxx - - help option
- **A dedicated service on the RB can renew automatically the proxy**
  - contacting the myproxy server

myproxy-init

```
[giorgio@glite-tutor:~]$ myproxy-init -s grid001.ct.infn.it
Your identity: /C=IT/O=GILDA/OU=Personal
   Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it
Enter GRID pass phrase for this identity:
Creating proxy
   ..................................................... Done
Proxy Verify OK
Your proxy is valid until: Sun Jun 19 21:18:27 2005
Enter MyProxy pass phrase:
Verifying password - Enter MyProxy pass phrase:
A proxy valid for 168 hours (7.0 days) for user giorgio now
   exists on grid001.ct.infn.it.
```

Principal option

- -c hours specifies lifetime of the credential stored
- -t hours specifies the maximum lifetime of credentials retrieved

myproxy-info

- **Useful to retrieve info on stored credentials**

  - [giorgio@glite-tutor:~]$ myproxy-info -s grid001.ct.infn.it
  - username: giorgio
  - owner: /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio Giorgio/Email=emidio.giorgio@ct.infn.it
  - timeleft: 167:55:34 (7.0 days)

myproxy-get-delegation

- This command can be used to retrieve a proxy stored,
- It is independent by the machine ! You don't need to have your certificate on board

```
[giorgio@glite-tutor:~]$ mv .globus dummy
[giorgio@glite-tutor:~]$ myproxy-get-delegation -s
   grid001.ct.infn.it
Enter MyProxy pass phrase:
A proxy has been received for user giorgio in
   /tmp/x509up_u513
```

```
mv dummy/ .globus
```

MyProxy and VOMS

- myproxy-init works creating a temporary plain proxy, with the “old” `grid-proxy-init`
- The plain proxy is stored on the MyProxy Server
- It will be valid for the desired duration (default is a week, maximum is the certificate lifetime)
- The proxy retrieved with `myproxy-get-delegation` will be a plain proxy too…..
- All the VOMS extensions in these way are lost
- Resources will rejects jobs from these user

- How can use delegated credentials keeping VOMS extension ?

Tricking the MyProxy server

This procedure is useful for those applications which needs to renew user credentials

- Store once a plain proxy on myproxy server

```
myproxy-init -s grid001.ct.infn.it
```

- Soon get the delegated credentials, specifying lifetime

```
myproxy-get-delegation -s grid001.ct.infn.it -t 27
Enter MyProxy pass phrase:
A proxy has been received for user giorgio in /tmp/x509up_u513
```

- Request a voms proxy signing it with the received delegation (no passphrase requested)

```
voms-proxy-init -t 25 -cert   /tmp/x509up_u513 -key
   /tmp/x509up_u513 -voms gildav
Your identity: /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it/CN=proxy/CN=proxy/CN=proxy/CN=proxy
Creating temporary proxy ............................... Done
/C=IT/O=INFN/OU=Host/L=CNAF/CN=cert-voms-01.cnaf.infn.it
/C=IT/O=INFN/CN=INFN Certification Authority
Creating proxy ..................................... Done
```

Problems

- These trick perfectly works on an uniform gLite testbed
- The most of testbeds is “hybrid”

(UI + RB glite, CE + WN lcg), or fully lcg

- The reason is already unknown, but seems dued to differences between CE’s, or to the ability of GSI to accept longs proxy chains (like the ones formed by VOMS + MyProxy)

Questions…